JITF Requirements Overview

Test Planning Oversight Committee

2 May 2001

Stephanie Ragusky
315-330-1785
DSN: 587-1785

JITF Test Focus

- Installation
  - Documentation review
  - Install application using PMO documents
- Integration
  - Confirm ability to share resources with other applications
- Security
  - Integration perspective only
  - Check audit settings, permissions, and ownerships
  - Check for presence of compilers or other development tools
  - In-depth security testing performed by DIA and designees
- Standards
  - Confirm that software complies with DoDIIS Profile of JTA

Areas of

- Test process addresses six major areas
  - Documentation (DOC requirements)
  - Installation (INST requirements)
  - Environment (ENV requirements)
  - Operations (OPS requirements)
  - User Interface (GUI requirements)
  - Security (SEC requirements)
- Sample JITF Integration requirements are provided to clarify the intent of each area

Documentation

- DOC-8
  - The IMA installation and configuration guide shall contain step by step instructions to perform IMA installation and configuration
    - Complete instructions are critical to efficient and successful installation of software. This is especially useful in easing the workload of administrators supporting multiple sites, which may have administrators of varying skill or experience levels
- DOC-20
  - The IMA configuration and installation guide shall specify the audit configurations (i.e., audit flags, etc.) that must be set in order to meet the system security requirements.
    - Providing information on audit configurations and information collected allows administrators to more effectively deal with site security requirements, and may also speed site acceptance test and certification process

Installation

- INST-4
  - The IMA shall not include bundled implementations of any standard network protocol
    - Specialized versions of standard network protocols may render a system vulnerable to exploitation or attacks. The Washington University FTP client (wuftp), for example, has recently been cited by security experts as a source of risk
- INST-3
  - The IMA shall not include bundled support applications
    - Provision of support applications such as file compression utilities, file viewers, etc. can clutter a server with duplicate copies and varying versions of a given utility or program. System administrators should be given the choice of using already-resident copies of required software to allow for simpler administration and upgrades

Environment

- ENV-7
  - IMA shall use the directory defined by the TMPDIR environment variable for all temporary files
    - Use of the standard temporary directory allows the administrator to more efficiently administer systems and networks. It also avoids the necessity of constantly monitoring a number of locations to prevent file systems from filling up and crashing the system
- ENV-4
  - The client application(s) of the IMA shall launch from the background menu or from an icon on the desktop
    - This allows administrators to provide users with standardized, simple access methods to launch applications. This reduces training loads and increases user productivity

Operations

- OPS-3
  - The execution environment that exists at the time of IMA launch shall not conflict with either the user’s overall operating environment or the execution environment of other applications
    - Resetting of a user’s current operating environment may cause instability in other applications and result in data and productivity losses
- OPS-23
  - Web pages shall not contain elements that obscure or interfere with reading clarity
    - Use of background images and similar graphics slows loading of pages and increases bandwidth requirements. In addition, it may render pages more difficult to use for readers with visual impairments such as color blindness

User Interf

- GUI-5
  - The IMA shall support cut and paste between windows
    - A user’s ability to cut and paste data between windows significantly enhances productivity
- GUI-2
  - The IMA shall allocate a private color map in order to avoid filling the default color map with non-shared, read/write color cells
    - Corruption of system color maps may cause screens or images to incorrectly display or, in some cases, be completely unusable

Security

- SEC-10
  - The IMA shall not implement audit collection or audit delivery functions
    - Implementation of audit collection functions increases the workload of both site administrators and security personnel in collecting and analyzing audit data
- SEC-8
  - IMA programs shall not be setuid or setgid to another user ID or group ID
    - Setting user or group ID incorrectly may introduce vulnerabilities and allow unauthorized users to view (or manipulate) data. In certain cases, it may also allow users to obtain elevated privileges or access to other programs not normally permitted to them

DoDIIS Prof

- Addressed by JITF Requirement DOC-30
  - Software compliance
    - Approved packages and versions
  - Utility and support programs
  - Confirm compliance with DoDIIS mobile code policies
  - Hardware compliance
    - Confirm that software works on supported hardware
- Timely incorporation of updates
  - Track changes and updates to DoDIIS Profile and incorporate into JITF test process
  - Disseminate information to customers through TPOC and other forums

How Are We Doing?

- Is JITF focus in line with site concerns?
- Possible areas of increased emphasis
  - Web (servers, browsers, standards)
  - Mobile code compliance
  - OS patches
  - Your suggestions???